Lecture 01

مقدمة عامة

تعريفات هامة

امنية الحاسوب computer security : اسم عام لمجموعة من الادوات المصممة لحماية البيانات واعاقة القرصنة الهكر.

امنية الشبكات network security :

مقياس او مقاييس حماية البيانات أثناء مرورها عبر الشبكة .

امنية الانترنت internet security :

مقاييس لحماية البيانات اثناء مرورها عبر مجموعة من الشبكات المتصلة مع بعضها .

خدمة الامنية security service

هي الاشياء المحسنة لأنظمة معالجة البيانات، ونقلها عبر المنظمات .

مقصودة لمقاومة الهجوم .

يتم تقديم الخدمة عبر واحدة او مجموعة من آليات الحماية/ الميكانزمات .

عادة يتم ربط الوظائف المكررة بوثائق مادية مثل :الحصول على توقيع مؤرخ، يحتاج إلى الحماية من الكشف . العبث. أو التخريب. يجب ان يكون موثقا (بشهادة) مسجلة ومرخصة .

security mechanism آليات الأمنية

الآلية المصممة للأعاقة والكشف والاصلاح من الهجمات المخلة بالأمنية.

لا توجد ألية واحدة تدعم جميع الوظائف المطلوبة .

هجمات الأمنية **security attack** أي حدث يهدد أمنية المعلومات المملوكة لمنظمة ما . :
تهدف امنية المعلومات إلى عرض كيفية منع هذه الهجمات او إفشالها .

خدمات الأمنية القياسية (**x.800**)

التحقق من الهوية **Authentication**: ضمان ان الجهة/الكائن المتصلة هي وحدها من تملك/تستحق هذه الميزة .

التحكم بالوصول **access control** : حماية الموارد من الاستخدام الغير مصرح به/ غير المخول .

سرية البيانات **data Confidentiality** هو حماية البيانات من الكشف الغير مصرح به .

سلامة البيانات **data integrity**: هو ضمان ان البيانات المستلمة هي ذاتها البيانات المرسلة من جهة مخولة بذلك **authorized**.

: عدم الانكار **Non-repudiation** الحماية من إنكار الحدث من قبل أحد طرفي الاتصال المرسل/المستقبل مثلا.

آليات معينة للحماية :

التشفير، التوقيع الالكتروني ، التحكم بالوصول، سلامة البيانات، تبادل الصلاحيات، المرور الزائد، التحكم بالمسار الشهادة القانونية.

تصنيف أنواع الهجمات التي تستهدف الامنية:

passive attacks :

1.الهجوم السلبي passive attacks

هو هجوم يتنصت ويراقب حركة المرور البيانات بغرض الحصول على محتوى الرسائل او مراقبة تدفق مرور البيانات.

2. الهجوم الايجابي active attacks

عملية تعديل قناة البيانات من أجل :

التنكر كجهة موثوقة امام الاخرين، إعادة تشغيل/ارسال بعض الرسائل، تغيير مسار الرسالة، إنكار الخدمة.

- **أمن المعلومات:** العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

عناصر أمن المعلومات:

- السرية **Confidentiality**
- المتكاملية **Integrity** النزاهة
- التوافر **Availability**

حماية المعلومات:

- البيانات: المعطيات الأولية قبل المعالجة Data
- المعلومات: المعطيات بعد المعالجة

التطور الزمني: منذ عصر الفراعنة وما قبلهم

حاجة الإنسان لحماية المعلومات: (فطرة انسانية، المحافظة على الخصوصية، حفظ الحقوق، التجارة، حقوق الآخرين....الخ)

- الحاجة الملحة مع عصر ثورة المعلومات والاتصالات: (العالم المفتوح، كثرة المتطفلين وحالات الاختراق، حالات التجسس، الحرب على الارهاب....).

المخاطر التي تهدد أمن المعلومات

الاختراق **Hacking**

Hackers :

- الاختراق الأولي
- يخترق دون أن يؤذي الشبكة أو الجاهز أو البيانات
- فقط يراقب ويطلع على المعلومات
- تعتبر خطوة أولى الاختراق التدميري

كالمواجهة

Crackers

- يخترق من أجل التخريب
- يحدث أثراً على النظام
- يغير على البيانات أو يعطل الأجهزة
- ممنوع بموجب القانون

طرق الحماية من المخاطر

- التشفير **Encryption**
- الحماية بالبرمجيات **SoftwareControl**
- الحماية بالأجهزة والمعدات **HardwareControl**
- السياسات الأمنية **SecurityPolices**
- الحماية التقليدية (الفيزيائية) **PhysicalSecurity**

- التشفير Encryption

- التشفير أو التعمية: عملية تحويل المعلومات من نص مقروء إلى صيغة غير مقروءة الا لمن يملك معرفة خاصة أو مفتاح خاص لإعادة تحويل النص المشفر إلى نص مقروء.
- فك التشفير : عملية استخدام المفتاح لإعادة النص المشفر إلى صيغته المقروءة الأصلية.
- علم التشفير Cryptography
- Crypto&Graphy وتعني الكتابة السرية
- Cipher أي جعل القيمة صفر ا أي بلا معنى ((صفر أو تصفير)) وتعني تشفير مأخوذة عن العربية

انواع التشفير

- التشفير الكلاسيكي (التقليدي) ClassicalEncryption
  - يعتبر من النوع التناظري
  - التبديل الحرف Substitution : تبديل الحرف بحرف آخر أو رمز أو رقم أو باكثر
  - إعادة ترتيب الأحرف Transposition : إعادة ترتيب الأحرف بمواقع مختلفة
- التشفير الحديث ModernEncryption
  - التشفير التناظري SymmetricEncryption
  - باستخدام مفتاح واحد (التشفير وفك التشفير باستخدام نفس المفتاح).
- التشفير اللامتناظر AsymmetricEncryption
  - باستخدام مفتاحين (التشفير يتم بمفتاح وفك التشفير يتم بمفتاح آخر).

Lecture 02

- التشفير بالطرق الكلاسيكيةClassical Method

الطرق الكلاسيكية هي الطرق القديمة التي استخدمت فيما مضى من قبل اختراع الحواسيب ، وبقيت الأساس لكثير من الخوارزميات الحديثة التي تستخدم اليوم ، حيث كانت تعتمد على أحلال أو أبدال حرف مكان أخر- ، والخوارزميات الجيدة كانت تقوم بالاثنين ، لكن جميع هذه الخوارزميات تعمل على الحروف فقط Character-Based أي على مدى 26 حرف ، بعكس الطرق الحديثة التي تعتمد على التعامل مع ال Bit (0 أو 1) ، وتقسم الطرق الكلاسيكية إلى قسمين رئيسين :

- شفرات التبديل Substitution Cipher :

في هذا النوع التشفير يكون عن تغيير أماكن حروف النص الأصلي ، أي مجرد تبديل في المواقع (بعض الكتب تطلق على هذا النوع اسم Permutation تقليب).

- شفره قيصر :Caesar Cipher

من أحد أشهر أنواع التشفير الكلاسيكي ، حيث تتميز ببساطتها ويعيبها سهولة كسر الشفرة الناتجة ببساطه ، وطريقة التشفير بأن نأخذ الحرف الأول من النص الأصلي ثم نقوم بجمع مفتاح مع النص الأصلي ، ويكون هو الحرف الأول في النص المشفر . وهكذا بالنسبة لباقي الحروف . وفي حال كان الحرف هو الحرف الأخير في الأبجدية نقوم بالرجوع إلي بداية الحروف (تكون على شكل دائرة) .

Plaintext letter	A	B	C	D	......	W	X	Y	Z
Ciphertext letter	D	E	F	G	....	Z	A	B	C

نأخذ مثال لتوضيح هذا النوع من الشفرات:

النص الأصلي :

FIRE MISSILE

نبدأ بعملية التشفير ، وكما ذكرنا كل حرف في النص الأصلي + المفتاح (3) ، وفي حالة تعدى الحرف Z نرجع من الأول.

الآن نقوم بأخذ الحرف الأول ونضيف إليه 3 حروف (الازاحة بمقدار 3 أحرف) ليكون:

F+3 = I

I+3 = L

ونكمل هكذا ، لباقي الحروف في النص الأصلي .

النص المشفر هو:

ILUH PLVVLOH

ولأن وضع الحروف المشفرة على نفس ترتيب الحروف في النص الأصلي يسهل من عملية تخمين الكلمة نقوم بوضع النص المشفر على شكل**block** أو مجموعات كل منها يتكون من 5 ، حروف (جرت العادة على ذلك ، لكن بالطبع يمكنك تغيرها).

الآن بعد وضع النص المشفر في شكل مجموعات كل منها يتكون من خمسة حروف يكون

الناتج:

ILUHP LVVLO H

وهكذا أصبح النص أكثر تعقيدا لكاسر الشفرة ، ولكنها تبقي خوارزمية قيصر ضعيفة للغاية .

العملية العكسية ، وهي فك التشفير ،هنا كل ما علينا هو طرح ثلاثة حروف من كل حرف في النص المشفر ، ليخرج إلينا النص الأصلي.

اذا نستنتج أن لكل خوارزمية تشفير مفتاح معين ، هذا المفتاح (في الطرق التقليدية ، التي هي في الأصل تندرج تحت خوارزميات التشفير بالمفتاح المتناظر

Cryptography Symmetric Key

يستخدم للتشفير ولفك التشفير ولذلك يجب أن يحفظ بمكان أمن . وفي حالة (شفره قيصر مفتاح التشفير هو 3 (أزاحة**Shift** بمقدار3)، بالطبع يمكن استخدام أي مفتاح أخر، لكنها لن تكون شفره قيصر.

- **كسر شفرة قيصر عن طريق التحليل الإحصائي FREQUENCY ANALYSIS**

جميع اللغات (سواء عربية أم انجليزية أم أي لغة أخرى) تحتوي على حروف تتكرر دائما وباستمرار في الجمل ، في اللغة العربية على سبيل المثال الحرف أ ، ل .. الخ ، أما في اللغة الإنجليزية فالحرE هو الحرف الأكثر تكرارا في الجمل.

الآن طريقة التحليل الإحصائي تعتمد على هذا الاحتمال ، فنقوم بالنظر في النص المشفر ونلاحظ الحرف الأكثر ترددا في النص ، بعدها قد يكون هذا الحرف في النص المشفر هو الحرف الأكثر تكررا في الجمل وهوE في اللغة الإنجليزية.

طبعا الاحتمال في الكثير من الأحيان يكون غير صحيح تماما ، ولكن يصلح في حال الطرق الضعيفة مثل شفره قيصر السابقة.

- **مثال:** لدينا الشفرة التالية ، ونريد كسرها وإرجاعها إلى حالتها الأصلية :

WFIDZ JVORT KCPVD GKZEV JJVDG KZEVJ JVORTKCPWF IDJFZ KZJNZ KYJVE
JRKZF EGVIT VGKZF EDVEK RCIVR TKZFE REUTF EJTZF LJEVJ JRCCK YZEXJ
RIVVJ JVEKZ RCCPV DGKPE FKSFI EEFKU VJKIF PVUEF KJKRZ EVUEF KGLIV
NZKYF LKCFJ JNZKY FLKXR ZEKYV IVWFI VZEVD GKZEV JJKYV IVZJE FWFID
EFJVE JRKZF EGVIT VGKZF EDVEK RCIVR TKZFE FITFE JTZFL JEVJJ EFVPV
VRIEF JVKFE XLVSF UPDZE UEFTF CFIJF LEUJD VCCKR JKVKE LTYFS AVTKF
WKYFL XYKEF JVVZE XREUJ FFEKF EFKYZ EBZEX EFZXE FIRET VREUE FVEUK
FZXEF IRETV EFFCU RXVRE UUVRK YEFVE UKFFC URXVR EUUVR KYEFR EXLZJ
YTRLJ VFWRE XLZJY TVJJR KZFEG RKYEF NZJUF DREUE FRKKR ZEDVE KJZET
VKYVI VZJEF KYZEX KFRKK RZEKY VSFUY ZJRKK MRCZM VJKYL JNZKY EFYZE
UIRET VFWDZ EUEFY ZEUIR ETVRE UYVET VEFWV RIWRI SVPFE UUVCL UVUKY
FLXYK IZXYK YVIVZ JEZIM RER

الخطوة الأولى هي معرفة الحرف الأكثر تكرارا ، ونظرا لطول الشفرة فيفضل عد كل حرف يتكرر ،

نبدأ بالعد ، نقوم بعد الحرف الأول وهو W ونلاحظ كم مره تكرر واحد ، اثنين ، ثلاثة ..... إلى أن نصل إلى نهاية الشفرة لنعرف أن الحرفW كرر 9 مرات نأخذ الحرف الثاني وهوF ونبدأ بالعد ، وهكذا مع باقي الحروف في الشفرة

نتيجة تكرار الحروف بعد العد:

A: 1 B: 1 C: 16 D: 14 E: 82 F: 69 G: 10 H: 0 I: 27 J: 47 K: 61
L: 15 M: 3 N: 5 O: 2 P: 8 Q: 0 R: 45 S: 5 T: 21 U: 28 V: 69
W: 9 X: 15 Y: 28 Z: 47

نلاحظ في النتيجة أعلاه. ، أن الحرف E هو الحرف الأكثر تكرارا في النص المشفر (تكرر 82 مره) ، الآن كما ذكرنا سابقا الحرف الأكثر تكرار في الشفرة قد يكون هو الحرفE ولأن في حالتنا هذه الحرف المشفر هو E اذا بالتأكيد الحرفE لن يكون هو الحرف البديل ، لذلك ، سوف نأخذ الحرف الأكثر تكرارا في الشفرة أتي بعد الحرف E .

الآن لدينا حرفين هما F,V . حيث تكرر كل منهم 69 مره ، وقد يكون أحدهم هو الحرف E

الآن نأخذ الحرفF ونشاهد الفرق بينه وبينE والنتيجة هي 1. (لأن الحرف F ، يأتي بعدE)

أيضا نأخذ الحرف الثاني هو V ونشاهد الفرق بينه وبين الحرف E والنتيجة هي 17 .

(الحرف V يأتي بعد17 حرف منE)

إلى هنا ، أصبح لدينا احتمالين ،

الأول هو أن يكون المفتاح هو 1 ، والثاني أن يكون المفتاح هو 17

نقوم بتجربة الأول ، ونطرح من كل حرف في الشفرة 1 (نرجع إلى الوراء بمقدار حرف) ،

النتيجة ستصبح غير مفهومه وبالتالي الازاحه بمقدار 1 خاطئة.

نجرب الازاحة بمقدار 17 ، وسوف نشاهد هذا النص:

FORMI SEXAC TLYEM PTINE SSEMP TINES SEXAC TLYFO RMSOI TISWI THSEN
SATIO NPERC EPTIO NMENT ALREA CTION ANDCO NSCIO USNES SALLT HINGS
AREES SENTI ALLYE MPTYN OTBOR NNOTD ESTRO YEDNO TSTAI NEDNO TPURE
WITHO UTLOS SWITH OUTGA INTHE REFOR EINEM PTINE SSTHE REISN OFORM
NOSEN SATIO NPERC EPTIO NMENT ALREA CTION ORCON SCIOU SNESS NOEYE
EARNO SETON GUEBO DYMIN DNOCO LORSO UNDSM ELLTA STETO UCHOB JECTO
FTHOU GHTNO SEEIN GANDS OONTO NOTHI NKING NOIGN ORANC EANDN OENDT
OIGNO RANCE NOOLD AGEAN DDEAT HNOEN DTOOL DAGEA NDDEA THNOA NGUIS
HCAUS EOFAN GUISH CESSA TIONP ATHNO WISDO MANDN OATTA INMEN TSINC
ETHER EISNO THING TOATT AINTH EBODH ISATT VALIV ESTHU SWITH NOHIN
DRANC EOFMI NDNOH INDRA NCEAN DHENC ENOFE ARFAR BEYON DDELU DEDTH
OUGHT RIGHT HEREI SNIRV ANA

الخلاصة:

- استخدام خوارزمية قيصر بتبديل الاحرف **Substitution**
- خوارزمية سهلة وبسيطة
- يمكن تفكيكها بسهولة فقط نحتاج إلى 26 محاولة في اسوأ الاحتمالات

- شفرات Monoalphabetic Substitution Cipher :

- فكرتها بسيطة وتعتمد على تبديل الأحرف الهجائية بشكل عشوائي
- على خلاف خوارزمية التي تعتمد تبديل الأحرف حسب طول المفتاح، لذا اذا تم معرفة حرف فان بقية الأحرف تصبح معروفة.
- فك التشفير، تعتمد على معرفة كل حرف وما يقابله في التوزيع العشوائي
- اذا تم معرفة فك تشفير حرف، فان بقية الأحرف تبقى غير معروفة

- التشفير Encryption

- يتم توزيع الأحرف الهجائية بطريقة عشوائية،

أمثلة

- قد نوزع **a** لتصبح (**x** أو **n** أو أ أي حرف أ خر)
- نوزع **b** لتصبح (**t** أو **r** أو أي حرف أخر باستثناء ما يقابل حرف **a** السابق)
- نكرر العملية على بقية ألأحرف مع مراعاة أن لايتم استخدام حرف سابق في التوزيع
- نستمر بتوزيع كافة أحرف اللغة حتى ننتهي منها
- على سبيل المثال لو قمنا بتوزيع الأحرف عشوائي وحصلنا على الترتيب التالي

حرف	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
توزيع	X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L	R	C	V	M	U	E	K	J	D	I

حرف	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
توزيع	X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L	R	C	V	M	U	E	K	J	D	I

- بعد توزيع الأحرف تتم عملية التشفير بشكل مباشر بتبديل كل حرف بالحرف المقابل له من الجدول
- مثال, لتشفير كلمة ALKAWARZMI
- نقوم بتبديل كل حرف بالحرف المقابل له من الجدول

A	L	K	A	W	A	R	Z	M	I
X	B	W	X	K	X	C	I	T	Z

- يصبح التشفير لكلمة ALKAWARZMI هو XBWXKXCITZ

- ملاحظات على الطريقة

- هذه الطريقة تعتمد على تبديل الاحرف **SubstitutionCipher** وتعتبر تقليدية
- لابد من توزيع جدول التشفير على طرفي الاتصال
- تمتاز بالسرعة في التشفير وفك التشفير(اليدوي و الآلي المحوسب).

- فك التشفير

- حتى نستطيع تفكيك التشفير لابد من معرفة جدول التشفير
- إن كان التشفير عبر الشبكة يتم ارسال جدول التشفير للطرف الآخر
- إن كان التشفير محلي (على **Hard Disk**) يقوم المُشَفِر بالاحتفاظ بجدول التشفير للمستقبل

جدول التشفير																										
حرف	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
توزيع	X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L	R	C	V	M	U	E	K	J	D	I

يقوم الطرف الذي يود تفكيك التشفير بإعادة ترتيب جدول التشفير لكن اعتماداً على صف التوزيع وليس صف الأحرف، ويتم الترتب لكامل العمود مع الجدول لنحصل على جدول فك التشفير التالي

جدول فك التشفير																										
توزيع	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
حرف	d	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f	j	q	n	m	u	s	k	a	c	i

- فك التشفير

- تفكيك التشفير يتم بشكل مباشر تحويل كل حرف مشفر من إلى ما يقابله من جدول فك التشفير

جدول فك التشفير

توزيع	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
حرف	d	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f	j	q	n	m	u	s	k	a	c	i

- لتفكيك النص المشفر **XBWXKXCITZ**
- نستخدم التبديل من جدول فك التشفير

X	B	W	X	K	X	C	I	T	[illegible]
A	L	K	A	W	A	R	Z	M	I

حصلنا على النص الأصلي وهو **ALKAWARZM**

Lecture 03

- شفره Simple Shift Vigenere Cipher

طريقة التشفير في هذا النوع من أبسط ما يكون ، حيث نقوم بتشفير الحرف الأول بالمفتاح الأول ، والحرف الثاني بالمفتاح الثاني ، وهكذا .. وفي حال انتهت المفاتيح أقوم بتكرار كتابتها مرة أخرى .

- مثال :

لدي هذه العبارة (النص الأصلي) :

DEFCON FOUR

أريد أن أشفرها بهذه الطريقة ، أول خطوه هي أن يكون المفتاح متغير ، أي مختلف من موقع لأخر.

مثلا قد يكون المفتاح على الشكل:

الحرف الأول في النص يشفر بالمفتاح : 5

الحرف الثاني يشفر بالمفتاح : 13

الحرف الثالث يشفر بالمفتاح : 2

الحرف الرابع يشفر بالمفتاح : 7

اذا المفاتيح (تسمى ب **Key Length**) في هذه الحالة هي : **5 13 2 7**

قبل أن نبدأ عملية التشفير ، نضع هذا الجدول لتسهيل معرفة مواقع الحروف:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

الآن نضع النص المراد تشفيره ، ومقابله نضع المفتاح ، ومن ثم نبدأ بعملية الازاحة ليخرج لدينا النص المشفر

نبدأ بالحرف الأول من النص الأصلي وهو D ، والمفتاح الأول هو 5

$$3 + 5 \bmod 26 = 8 = I$$

وهكذا لباقي الحروف في النص....

هذه الصوره توضح عملية التشفير ، السطر الأول هو النص الأصلي ، السطر الثاني المفاتيح ،

وفي حال انتهت نعيد كتابتها مره أخرى ، السطر الأخير هو الناتج من جمع السطر الأول مع الثاني وهو النص المشفر:

~~Plaintext~~	D	E	F	C	O	~~N~~	F	O	U	R
Shift value	5	13	2	7	5	13	2	7	5	13
Ciphertext	I	R	H	J	T	A	H	V	Z	E

الآن نأخذ الناتج ونضعه في شكل**Block** كل منها يتكون من 5 حروف

اذا النص المشفر هو:

IRHJT AHVZE

ملاحظة:

يمكن استخدام نص أو جملة بدل هذه الأرقام ، وعند التشفير أعوض بكل حرف من هذه الجملة بالرقم على حسب موقعها.

هنا في هذه الطريقة بعدما أختار الجملة (مفاتيح التشفير) ، يكون التشفير عن طريق أخذ الحرف الأول من النص الأصلي مع الحرف الأول من جملة التشفير وأخذ نقطة التقاطع في جدول التشفير a tabular recta ،

والجدول شكله كما هو واضح في الشكل التالي:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

الآن مثلا لدينا النص التالي:

HARKONNEN RULZ

وأريد أن أشفره باستخدام هذه الجملة SPICE :

أقوم في البداية بأخذ نقطة التقاطع بين الحرف الأول في النص الأصلي والحرف الأول في الجملة .

جميع الأعمدة تمثل الحروف في النص الأصلي ، السطور تمثل الحروف في جملة التشفير.

لينتج لدينا النص المشفر ZPZMSFCMPVMAH :

وأقوم بفصلهم كل خمسة حروف على حده ZPZMS FCMPV MAH :

ولفك التشفير ، نقوم بالعملية العكسية ، وفي هذه الحالة تكون الأعمدة هي النص الأصلي ، والسطور هو المفاتيح (نفس طريقة التشفير) ، ولكن لكي أفك تشفير حرف ما ، أولا أخذ الحرف الأول من جملة التشفير ، وأبحث في السطر الخاص بالحرف الأول من جملة التشفير عن الحرف المشفر الأول ، وعندما أجده يكون الحرف الموجود في العامود هو الحرف الأصلي.

مثال لتوضيح عملية فك التشفير :

فك تشفير العبارة ZPZMSFCMPVMAH :

عن طريق الجملة SPICE :

HARKONNEN RULZ

- شفره فجينير تلقائية المفتاح THE AUTO-KEY VIGENERE CIPHER

شفرات فجينير بأنواعها المختلفة متشابهة فيما بينها بشكل كبير ، لكن يوجد فرق واضح بين كل نوع أخر ، في شفره فجينير تلقائية المفتاح ، التشفير يكون بنفس الطريقة ، وجملة التشفير أيضا ، لكن في حال انتهت جملة التشفير وحتى نتجنب تكرر المفتاح بعد انتهائه نقوم بوضع النص الأصلي ، أي أن النص الأصلي يدخل في عملية التشفير.

- مثال

LIGHT SPEED CHEWIE NOW

بالمفتاح (جملة التشفير ، المفاتيح ، كلها نفس المعنى) التالي**ARGH** :

أول خطوه نقوم بها هي تشفير الحرف الأول في النص الأصلي مع الحرف الأول في جملة التشفير

L + A = L

I + R = Z

G + G = M

H + H = O

إلى هنا نلاحظ انتهاء المفاتيح (وبدل من إعادته مره ثانية كما حدث في الطريقة السابقة) نقوم بإدخال النص الأصلي كمفتاح

L الحرف الأول من النص الأصلي

L + T =E

I الحرف الثاني من النص الأصلي

I + S = A

وهكذا إلى أن ننتهي من تشفير النص.

ويفضل دائما كتابة النص ، والمفتاح ، والنص المشفر ، بهذه الطريقة للتسهيل :

Plaintext	L	I	G	H	T	S	P	E	E	D	C	H	E	W	I	E	N	O	W
Key	A	R	G	H	L	I	G	H	T	S	P	E	E	D	C	H	E	W	I
Ciphertext	L	Z	M	O	E	A	V	L	X	V	R	L	I	Z	K	L	R	K	E

ولفك التشفير ، نقوم بفك الحرف الأول من النص المشفر مع المفتاح الأول ، والحرف الثاني من النص المشفر مع المفتاح الثاني ... ونستمر هكذا إلى أن تنتهي المفاتيح.

ولكي نقوم بفك الحرف المشفر التالي (بعد انتهاء المفاتيح) ، نقوم بفك تشفير الحرف المشفر مع المفتاح (الذي يكون عبارة عن أول حرف أصلي حصلنا عليه بعد أول عمليه فك تشفير) . أي أن المفتاح (بعد انتهاء المفاتيح) يكون هو الحرف الأصلي الذي حصنا عليه ، وبعدها يكون الحرف الأصلي الثاني الذي حصنا عليه . (أي أن النص الأصلي يكون هو المفتاح) .

- شفره فجينير طويلة المفتاح THE Running KEY VIGENERE CIPHER

هنا في هذا النوع من الشفرات ، يجب اختيار جملة تشفير(مفاتيح) بحيث تكون أطول من النص الأصلي (لاحظ اسم الشفرة) ، وأخذ هذه الجملة ممكن يكون من كتاب ما أو مجلة أو أي نص طويل ، يجب أيضا أن تكون موجودة عند الطرف الأخر ، أو اختيار أي جملة للتشفير وإرسالها إلى الطرف الأخر (المهم أن تكون طويلة).

مثال ، أريد تشفير النص التالي TORA TORA TORA :

بجملة التشفير التالية :

AND GOD SAID LET THERE BE LIGHT

لاحظ الجملة أطول من المفتاح ، وطريقة التشفير تكون عادية كما كنا نشفر من قبل.

النتيجة بعد التشفير:

Plaintext	T	O	R	A	T	O	R	A	T	O	R	A
Key	A	N	D	G	O	D	S	A	I	D	L	E
Ciphertext	T	B	U	G	H	R	J	A	B	R	D	E

وفك التشفير هو العملية العكسية ، وبنفس الأسلوب .

- أسطوانة جيفيرسون THE JEFFERSON CYLINDER

اسطوانة جيفيرسون واحده من أقوى الأجهزة التي استخدمت في التشفير، حيث الشفرة الناتجة قوية ولا يمكن كسرها بسهولة أبدا ، إلا في حالة سرقة الجهاز بأكمله ، الاسم جيفيرسون يعود إلى اسم مخترعها توماس Thomas Jefferson.

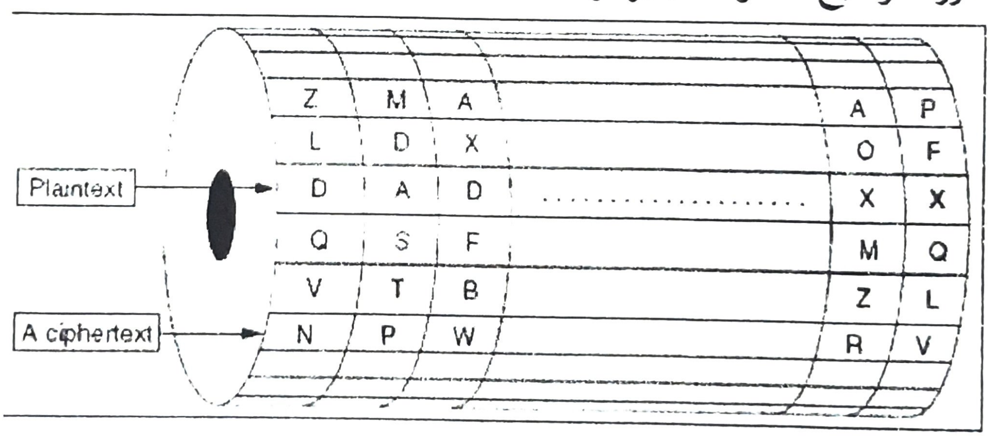
هذه الإسطوانه تتكون من 36 عجله بجانب بعض ، و 26 صف ، أي أن كل صف به 36 عجله (حرف) .

في حال أردت التشفير النص الأصلي ، يجب أن أضع جميع العجلات في صف ما في شكل النص الأصلي ،أي أقوم بتحريك العجلة الأولى مثلا في الصف الرابع إلى الحرف المراد ، الآن أحرك العجلة الثانية في نفس الصف إلى الحرف الثاني المراد تشفيره ، ونفس الكلام لباقي الحروف لكن في نفس الصف.

الآن بعد وضع الصف كامل على النص الأصلي ، أقوم باختيار أحد ال 25 صف المتبقية ، أي هناك 25 شفره ممكنه، وأرسل هذا النص للطرف الأخر.

في حالة فك التشفير ، يقوم بترتيب النص المشفر في صف ، بعدها ينظر إلى باقي ال 25 صف ويشاهد من هو النص الأصلي ، أي يقوم بالبحث في جميع هذه الصفوف ، حتى يستطيع الحصول على النص الأصلي .

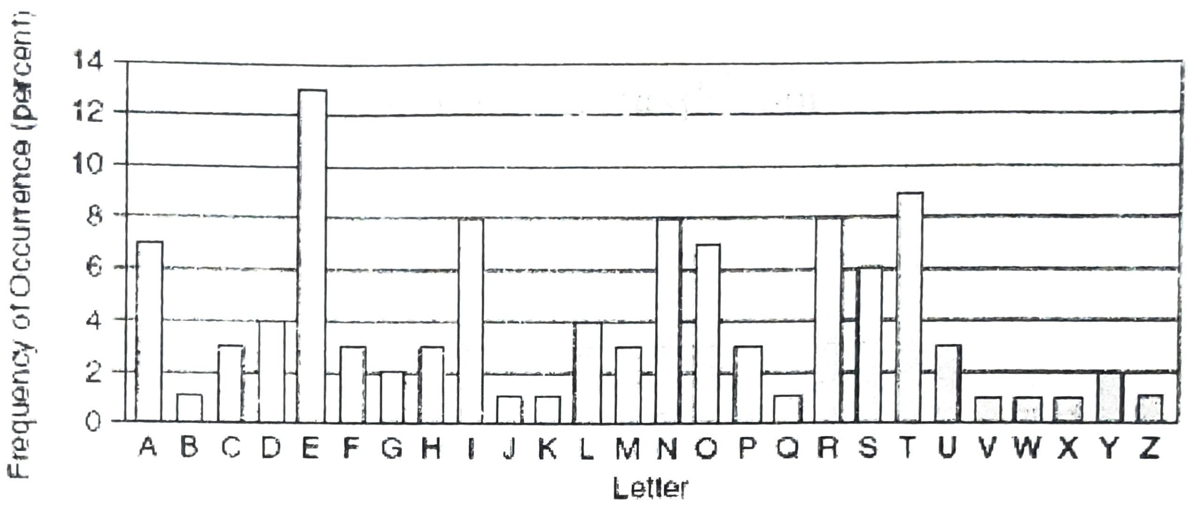
صوره لتوضيح أسطوانة جيفيرسون:



- التشفير بطريقه الHOMOPHONIC SUBSTITUTION CIPHERS

تعتبر طريقة ال**HOMOPHONIC** من الطرق الجيدة لإحباط التحليل الإحصائي ، الذي لن يستطيع فعل شيء لمثل هذا النوع من الشفرات ، حيث كما نعرف أنه هناك حروف تتكرر أكثر من غيرها في اللغة ، في هذه الطريقة كل حرف من هذه الحروف التي تتكرر كثيرا ، يكون لها أكثر من احتمال ، أي تتشفر إلى أكثر من حرف وبطريقة عشوائية.

أنظر لهذا الجدول



أنظر إلى جدول الHomophonic

Plaintext letter	Choices for ciphertext unit												
A	BU	CP	AV	AH	BT	BS	CQ						
B	AT												
C	DL	BK	AU										
D	BV	DY	DM	AI									
E	DK	CO	AW	BL	AA	CR	BM	CS	AF	AG	BO	BN	BE
F	BW	CM	CN										
G	DN	BJ											
H	AS	CI	CK										
I	DJ	BI	AX	CJ	AB	BP	CU	CT					
J	BX												
K	DI												
L	AR	BH	CL	AJ									
M	DH	BG	AY										
N	BY	DG	DF	CH	AC	BR	DU	DT					
O	DZ	BF	DX	AK	CG	BQ	DR						
P	BZ	DE	AZ										
Q	DD												
R	AQ	DC	DQ	AL	CE	CF	CV	DS					
S	AP	AN	AO	CD	DW	DV							
T	CB	DB	DP	CC	AD	CY	CW	CX	AE				
U	CA	AM	BA										
V	BB												
W	CZ												
X	BD												
Y	DO	DA											
Z	BC												

مثلا ، أريد تشفير العبارة:

RETREAT

، نبدأ بالحرف الأولR له أكثر من 8 شفرات في الجدول ، ويمكنك اختيار ما تشاء.

الحرف الثاني E له13 شفره ، ويمكنك اختيار ما تشاء. ،

الآن وبعد أن قمت بالتشفير ، الناتج هو

DQ AW CC AQ CO BS DB

(الناتج قد يختلف عن الناتج الخاص بك ، لأنني قد اخترت شفرات لم تختارها) .

ولفك التشفير ، يمكنك بناء جدول عكسي **inverse mappings** للجدول السابق ، كما في الشكل التالي:

Ciphertext Pair	Letter	Ciphertext Pair	Letter	Ciphertext Pair	Letter	Ciphertext Pair	Letter
AA	L	BA	U	CA	U	DA	Y
AB	I	BB	V	CB	T	DB	T
AC	N	BC	Z	CC	T	DC	R
AD	T	BD	X	CD	S	DD	O
AE	T	BE	E	CE	R	DE	P
AF	E	BF	O	CF	R	DF	N
AG	E	BG	M	CG	O	DG	N
AH	A	BH	L	CH	N	DH	M
AI	D	BI	I	CI	L	DI	K
AJ	L	BJ	G	CJ	I	DJ	I
AK	C	BK	C	CK	H	DK	E
AL	H	BL	L	CL	H	DL	C
AM	U	BM	E	CM	F	DM	D
AN	S	BN	E	CN	F	DN	G
AO	S	BO	E	CO	E	DO	Y
AP	S	BP	I	CP	A	DP	T
AQ	R	BQ	O	CQ	A	DQ	R
AR	L	BR	N	CR	E	DR	O
AS	H	BS	A	CS	E	DS	R
AT	B	BT	A	CT	I	DT	N
AU	C	BU	A	CU	I	DU	N
AV	A	BV	D	CV	R	DV	S
AW	F	BW	F	CW	T	DW	S
AX	I	BX	J	CX	T	DX	O
AY	M	BY	N	CY	T	DY	D
AZ	P	BZ	P	CZ	W	DZ	O

وهو نفسه الجدول السابق ، لكن تم وضع أي شفره في صف لكل شفره ، وما يقابلها من النص الأصلي . ويصبح فك التشفير أمر في غاية السهولة!

وبالرغم من قوه هذه الطريقه وشفراتها الأمنه ، الإ إنـها لم تستخدم بشكل كبير ، لأنـها كما لاحظنا تعتمد على اللغة ، والحروف التي تتكرر فيـها كثيرا ، على عكس الشفرات الحديثة التي لا تعتمد إطلاقا على اللغة.

Lecture 04

- خوارزمية بلاي - فير PlayfairCipher

مخترعها هو العالم البريطاني تشارلز ويتس تون سنة 1854 وسميت باسم صديقه

السيد(بلاي – فاير)

- استخدمت في الحرب العالمية الأولى والثانية
- كان يستخدمها الرئيس الأميركي جون كينيدي
- لتضييع خصائص اللغة يستخدم تشفير الحرف بناء ا على ارتباطه بحرف أ خر
- لهذا السبب قد يكون تشفير حرف a هو h وفي المرة القادمة s وفي التي يليها t وهكذا

- التشفير Encryption

نقوم بوضع كل حرفين مع بعض

- غير مسموح تكرار الأحرف المتتابعة مثل Hello تصبح هكذا He lx lo
- يجب أ أن يكون عدد الحرف زوجي أي كل حرفين يشكلان وحدة واحدة
- ان كان عدد الأحرف فردي نضيف x على أخر حرف

- مرحلة بناء مصفوفة التشفير

- نستخدم الأحرف اللتينية في مصفوفة خماسية Matrix
- نلغي أحد الحرف ويدمج مع حرف أ خر)بلعادة I/J (يشكلان حرفا واحدا)
- نحدد مفتاح التشفير ويكتب في بداية المصفوفة (حرف في كل خلية مع عدم تكرار الحرف)

• توزيع باقي الأحرف الهجائية على ما تبقى من خلايا المصفوفة (مع ملاحظة أ أن الحرف يجب أن لا يتكرر).

A	B	C	D	E
F	G	H	I / J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

اختيار مفتاح التشفير و اعادة بناء المصفوفة

• افرض المفتاح هو كلمة **MONARCHY**

• نقوم بكتابة المفتاح في بداية المصفوفة

• نستكمل بقية الأحرف الهجائية والتي لم توجد في المفتاح

• نقوم بتوزيع المفتاح على الطرف الأخر بالاتصال

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

- ألية التشفير

- نأخذ كل حرفين مع بعض
- ننظر الحرف من الجدول (مكان تقاطع الحرف الأول مع الثاني في الجدول)
- يتم تبديل كل حرف بالحرف المقابل في التقاطع من نفس السطر
- ان كان الحرفان على نفس السطر يتم تبديل كل حرف بالحرف الذي يلية على جهة اليمين مع تبديل أخر حرف بالسطر مع أول حرف بنفس السطر
- ان كان الحرفان على نفس العمود يتم تبديل كل حرف بالحرف الذي أسفل منه مع تبديل أ خر حرف بالعمود مع أ أول حرف بنفس العمود
- نكرر العلمية حتى نهاية أحرف الكلمة

- مثال

المفتاح لا يحتوي على أحرف مكررة افرض المفتاح هو كلمة MONARCHY

- نقوم بكتابة المفتاح في بداية المصفوفة
- نستكمل بقية الأحرف الهجائية والتي لم توجد في المفتاح
- نقوم بتوزيع المفتاح على الطرف الآخر بالاتصال

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

- مثال

المفتاح يحتوي على أحرف مكررة

- افرض المفتاح هو كلمة BALLOON
- نقوم بكتابة المفتاح في بداية المصفوفة مع شطب الأحرف المكررة
- نستكمل بقية الأحرف الهجائية والتي لم توجد في المفتاح
- نقوم بتوزيع المفتاح على الطرف الآخر بالاتصال

B	A	L	O	N
C	D	E	F	G
H	I	K	M	P
Q	R	S	T	U
V	W	X	Y	Z

- تبديل مواقع الأحرف Transposition/PermutationCipher

يعتمد هذا النوع على اعادة ترتيب الأحرف الكلمة بطريقة تحقق الشروط التالية

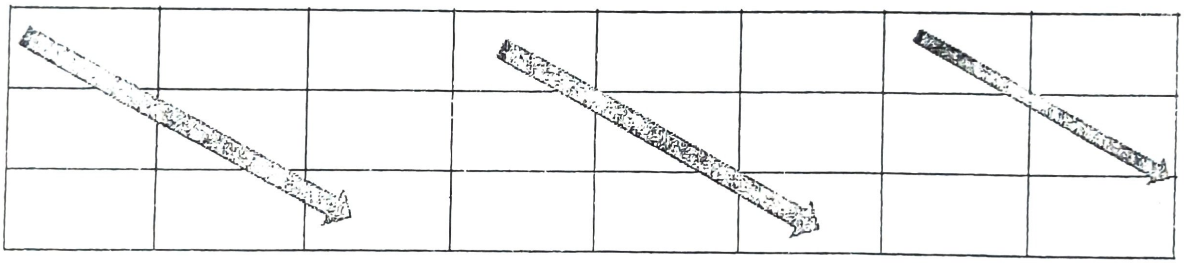
- نستخدم نفس الأحرف دون اجراء تغيير عليها
- نعيد ترتيب الأحرف بحيث يختفي معنى الكلمة الأصلي (وهذا يشكل عملية التشفير)
- عملية اعادة ترتيب الأحرف يجب أن تكون قابلة للاسترجاع (أي يجب أن نستطيع اعادة تشكيل الكلمة الأصلية)(وهذا يشكل عملية فك التشفير).
- لا مانع من اضافة بعض الأحرف في حالات خاصة لنجاح كتابة العملية

- خوارزمية(عامود السياج)(RailFence)

- تسمى كذلك خوارزمية **ZigzagCipher**
- ~~طريقة سهلة~~ وسريعة ويمكن تنفيذها يدو يا
- يمكن تفكيكها بسهولة
- تستخدم في التشفير البسيط، ولكن يمكن استخدامها كأداة لتشتيت النص

التشفير في خوارزمية(عامود السياج) **RailFence**

- نكتب النص الذي نريد تشفيره على عدد من الأسطر نحددة مسبقا ونعتبرة (مفتاح التشفير)
- نكتب النص بشكل قطري على الصفوف
- نكتب النص المشفر بحيث نضع الصف الأول ثم الصف الثاني وهكذا
- ولكن يمكن معالجتها (في الخوارزمية الأصلية) ملاحظة لايتم اعتبار الفراغات في الكلمة



- مثال

- لتشفير عبارة (اقرأ باسم ربك) باستخدام صفين(عدد الصفوف =2)

ا		ر		ب		س		ر		ك		
	ق		أ		ا		م		ب			

- لكتابة النص المشفر، نقرأ الصف الأول ثم الصف الثاني

1	ا		ر		ب		س		ر		ك		
2		ق		أ		ا		م		ب			

- النص المشفر هو اربسركقاأمب

- مثال

لتشفير عبارة (اقرأ أ باسم ربك) باستخدام (عدد الصفوف = 3)

1	ا			أ			س			ب			
2		ق			ب			م			ك		
3			ر			ا			ر				

النص المشفر هو أسبقبمكرار

- فك التشفير

- نقوم بتقسيم طول الكلمة على عدد الصفوف

- نقسم الكلمة إلى جزئين, الجزء الأول هو الأطول = 6 أحرف, والصف الثاني يكون 5 أحرف,
11=5+6 قامب
- نشكل النص الأصلي كالتالي
- نأخذ الحرف الأول من الجزء الأول والحرف الأول من الجزء الثاني(اق) قامب
- ثم نأخذ الحرف الثاني من الجزء الأول, ثم الحرف الثاني من الجزء الثاني(اقرأ) ار
- ونكرر هكذا حتى ينتهي النص المشفر

- ملاحظات على الخوارزمية

- تعتبر ضعيفة لو استخدمت لوحدها
- يمكن تنفيذها يدوي باستخدام قلم و ورقة بكل سهولة
- يفضل استخدامها بعد أو قبل استخدام احدى طرق التشفير التقليدية (التبديل)
- ممكن تكرار عمليات التشفير لأكثر من مرة لتقوية النص المشفر
- الأحرف سوف تبقى كما هي (أي أن نسبة تكرار الأحرف من خصائص اللغة تبقى موجودة.

- الشفره الأمنه THE ONE-TIME PAD

هذه الشفره هي الشفره الأكثر أمانا على مدى تاريخ التشفير ، لم ولن يستطيع أحد كسر شفرات هذا النوع أبدا ، واستخدمت هذه الشفرات في الكثير من الحكومات وأجهزه الاستخبارات.

طريقة الشفره كالتالي ، **هو عمل الكتاب one-time pad** (مثلا نطلق عليه) بداخل هذا ، كتاب توجد صفحات **Sheets**

بداخل كل صفحة من هذه الصفحات أرقام عشوائية لا تتكرر أبدا ، هذه الأرقام العشوائية تمثل الازاحة المستخدمة (أي كل رقم منها هو مفتاح) .

في حال شفرت نص بهذه الطريقة أقوم بإرسال النص المشفر و رقم الصفحة إلى الطرف الأخر وأقوم بقطع الصفحة من الكتاب وأحرقها بالنار ، اذا لزم الأمر أي يتم القضاء عليها.

والطرف الأخر يكون لديه نسخة مماثلة من الكتاب **one-time pad** ويقوم بفك التشفير عن .

طريق رقم الصفحة ، و بعدما يتم فك التشفير والحصول على النص الأصلي ، يتم أيضا قطع الصفحة أيضا

مثال ، لدي الشفره التالية **ENGAGE WARP DRIVE** :

والصفحة الأولى تتكون من:

23 10 16 18 6 2 24 7 8 8 0 25 7 4 25 12 25 5 9 19 13 1 21 0 13 20 9

15 4 19 0 0 8 3 17 22 22 6 13 12 11 5

أقوم بجمع الحرف الأول **E** مع الرقم الأول **9** لينتج **N** و أجمع الحرف الثاني **N** مع الرقم الثاني **20** لينتج **H** وهكذا..... .

اذا تبقت أرقام في الصفحة ، أو لم تبقى هناك أي أرقام ، أقوم بتدمير الصفحة ،

Plaintext letter	E	N	G	A	G	E	W	A	R	P	D	R	I	V	E						
Shift value	9	20	13	0	21	1	13	19	9	5	25	12	25	4	7	25	0	8	8	7	24
Ciphertext letter	N	H	T	A	B	F	J	T	A	U	C	D	H	Z	L						

Plaintext letter																					
Shift value	2	0	18	16	10	23	5	11	12	13	6	22	22	17	3	8	0	0	19	4	15
Ciphertext letter																					

باقي الارقام في الصفحه ، لا تستخدم

وهكذا نلاحظ أنه يستحيل كسر الشفره هنا ، لأن المفتاح عشوائي ولن يتكرر أبدا ، وفي هذه الحالة لن يتم كسر الشفره.

هذه الطريقه لن تستخدم هذه الأيام بسبب صعوبة الاحتفاظ ب هذا الكتاب ، وصعوبة إرسالها إلى الطرف الأخر ، أيضا صعوبة أضافة صفحات جديدة فيه.

Lecture 05

- الأساسيات Preliminaries

لفهم أغلب الشفرات الحديثة يلزم فهم الكثير من نظرية الأعداد Number Theory

اذا كان لدينا عددين صحيحين a و b ، وكان a != 0 (لا يساوي 0) . نقول عن a يقسم b اذا كان لدينا عدد ثالث c بحيث b = a*c . اذا كان a يقسم b نشير إليه بالرمز a|b .

مثال:

27 | 3 صحيح. لان 27 = 9* 3 ،

32 | 5 غير صحيحة لأن 32 =5*c ولا توجد عدد صحيح يحمل مكان c ،

اذا كان لدينا ثلاثة أعداد صحيحة x,y,z ، وكان x|y و y|z اذا x|z .

مثال :

لدينا 9 | 3 ، و 72 | 9 ، اذا 3 تقسم 72 = 72 | 3

الأعداد الأولية Prime Number :

تلعب الأعداد الأولية تلعب دورا كبيرا جدا في التشفير وخاصة في الطرق الحديثة ، وتعريفها كالتالي :

العدد الأولي ، هو العدد الصحيح integer أكبر من 1 ،ولا يقبل القسمة إلا على نفسه وعلى 1 . باقي الأعداد التي أكبر من 1 وغير أوليه تسمى أعداد مركبه Composite Number

مثال على أعداد أوليه:

2و 3 و 7 و 23 و 29 و 163 والكثير غيرها .

مثال على أعداد مركبة :

4 (حيث أنها تقبل القسمة على 2)

100 (تقبل القسمة على 2 و 5)

مثال على أعداد غير أوليه وغير مركبة

0 و 1 وجميع الأعداد السالبة ، مثل – 21.

جميع الأعداد الصحيحة التي أكبر من 1 ، لها قاسم أولي .
الأعداد الأولية غير منتهية .
اذا كان لدينا عدد صحيح مركب N ، اذا يكون لدى n قاسم أولي لا يتعدى الجذر التربيعي لN .

وهذا معناه اذا أردنا أن نعرف على العدد x هو أولي أم لا ، سوف نبحث من البداية 2 (لان واحد ليس أولي) إلى أن نصل إلى جذر العدد x ونختبر كل عدد من هذه الأعداد ، هل يقبل . x القسمة عليها ، في حال تحقق ذلك ، نكون قد عرفنا أن العدد ليس أولي ، وإذا لم يتحقق فيكون العدد أولي.

مثلا لدينا العدد 101 ، نبدأ بالاختبار من 2 ، إلى جذر 101 وهو 10

هل 101 يقبل القسمة على 2 . لا

هل 101 يقبل القسمة على 3 ، لا

هل 101 يقبل القسمة على 4 و 5 و 6و 7 و 8 و 9 . إلى أن نصل إلى 10 ، وأيضا لا يقبل ، اذا النتيجة أن العدد 101 هو عدد أولي.

القاسم المشترك الأعظم (اختصارا Greatest Common Divisor (GCD

القاسم المشترك الأعظم لعددين هو أكبر عدد صحيح يقبل القسمة على العددين .

مثلا نريد معرفة القاسم المشترك الأكبر للعددين 30،18 . نقوم بمعرفة جميع قواسم العددين ، ونأخذ العدد الأكبر من هذه القواسم :

30 يقبل القسمة على 1 و 2 و 3 و 5 و 6 و 10 و 15 و 30

18 يقبل القسمة على 1 و 2 و 3 و 6 و 9 و 18

. نلاحظ في الأعداد السابقة أكبر قاسم يقبل القسمة على العددين وهو 6

GCD(30,18) = 6

يقال عن عددين "أوليان فيما بينهما" Relatively Prime اذا كان القاسم المشترك الأعظم لهم هو 1 .

: الأزواج التالية من الأعداد أوليان فيما بينهما Relatively Prime

. 8 و 9 ، لأن القاسم المشترك الأعظم لهم هو 1

23 و 44

27 و 55

الاشاره السالبة لا تؤثر في حساب القاسم المشترك الأعظم :

GCD(x,y) = GCD(x,-y) = GCD(-x,y) = GCD(-x,-y) = GCD(|x|,|y|)

مثال :

GCD(18,-54) = GCD(18,54) = 9

لأخذ القاسم المشترك الأعظم لمجموعه من الأعداد نقوم بأخذ القاسم المشترك الأعظم لعددين منهم ، والناتج نأخذه مع العدد الثالث وهكذا .

مثال : القاسم المشترك الأعظم ل : 20 و 30 و 15 هو 5 وذلك :

GCD(20,30) = 10

CGD(10,15) = 5

اذا كان القاسم المشترك الأعظم لمجموعه من الأعداد = 1 ، وكان هناك زوج من هذه الأعداد (أي عددين) القاسم المشترك الأعظم هو غير 1 (أي ليس أوليان فيما بينهما) ، فأنها تسمى mutually relatively prime ، أما في حالة كان جميع الأزواج مع بعضها يكون القاسم يساوي واحد فإنها تسمى pairwise relatively prime .

مثال : لحساب القاسم المشترك الأعظم للأعداد 28 و 126 و 21 و 10

((28,126) ، 21 ، 10) =

(14 ، 21 ، 10) =

((14,21) ، 10) =

(7,10) =

1 =

لاحظ النتيجة هي واحد ، بالرغم من أن هناك زوج من الأعداد غير أوليان فيما بينهما ، (28,126) =14 .

وفي هذه الحالة تسمى مجموعه الأعدادmutually relatively prime أما في حالة كان جميع الأزواج من الأعداد أوليان فيما بينهما فتسمى مجموعه الأعداد ب

pairwise relatively prime

مثال :القاسم المشترك للأعداد 18 و 9 و 25 هو 1 ، ومع ذلك فهي

mutually relatively prime

لان القاسم المشترك الأعظم ل 18,9 هو 9 (أي هما ليسا أوليان فيما بين هما) .

. مثال:

أوجد القاسم المشترك الأعظم GCD(93,36)

GCD(93,36) = GCD(36,93 mod 36) = GCD (36,21)

GCD(36,21) = GCD(21,36 mod 21) = GCD (21,15)

GCD(21,15) = GCD(15,21 mod 15) = GCD (15,6)

GCD(15,6) = GCD(6,15 mod 6) = GCD (6,3)

GCD(6,3) = GCD(3,6 mod 3) = GCD (3,0)

GCD(93,36) = 3

خوارزمية أقليدس Euclidean Algorithm

من الممكن أن نستخدم الطريقة التالية لحساب القاسم المشترك الأعظم:

GCD (A1,B1)=

$A1 = B1 * Q1 + R1$

$A2 = B2 * Q2 + R2$

$A3 = B3 * Q3 + R3$

$A4 = B4 * Q4 + R4$

. . . .

. . . .

$An = Bn * Qn + Rn$ 1

GCD (A1,B1) = Bn

حيث أن A1 المقسوم عليه

B1 القاسم

Q1 ناتج القسمة

R1 باقي القسمة

مثال:

أوجد القاسم المشترك الأعظم بين الرقمين GCD((1970,1066

1970 = 1066 * 1 + 904 .... GCD(1970,1066)

1066 = 904 * 1 + 162 .... GCD(1066,904)

904 = 162 * 5 + 94 .... GCD(904,162)

162 = 94 * 1 + 68 .... GCD(162,94)

94 = 68 * 1 + 26 .... GCD(94,68)

68 = 26 * 2 + 16 .... GCD(68,26)

16 = 10 * 1 + 6 .... GCD(16,10)

10 = 6 * 1 + 4 .... GCD(10,6)

6 = 4 * 1 + 2 .... GCD(6,4)

4 = 2* 2 + 0 .... GCD(4,2)

GCD(1970,1066) = 2 ← Bn

المضاعف المشترك الاصغر (Least Common Multiple)(LCM)

1- المضاعف المشترك الأصغر هو أصغر عدد موجب يقبل القسمة على عددين بدون باقي ويتم احتسابه بالمعادلة التالية:

$$LCM(a, b) = |a * b| / GCD(a, b)$$

مثال: أوجد LCM(4864,3458)

GCD(4864,3458)

$$4864 = 3458 * 1 + 1406$$

$$3458 = 1046 * 2 + 646$$

$$1406 = 646 * 2 + 114$$

$$646 = 114 * 5 + 76$$

$$114 = 67 * 1 + 38$$

$$76 = 38 * 2 + 0$$

$$GCD(4864,3458) = 38$$

$$LCM(3864,3458) = |3864 * 3458| / GCD(4864,3458)$$

$$= 16819712 / 38$$

$$= 442624$$

2- الطريقة الاعتيادية تعتمد على تحليل كل رقم إلى عوامله الأولية ومن ثم اخذ حاصل ضرب أعلى قوة مشترك والعوامل غير المشتركة.

مثال:

أوجد LCM(4864,3458)

2	3458
7	1729
13	247
19	19
	1

2	4864
2	2432
2	1216
2	608
2	304
2	152
2	76
2	38
19	19
	1

$4864 = 2^8 * 19$

$3458 = 2 * 7 * 13 * 19$

$LCM(4864,3458) = 2^8 * 7 * 13 * 19$

$= 442624$

مثال:

أوجد LCM(93,364)

LCM(93,36) = |93 * 36| / GCD(93,36)

= 3348 / 3

= 1116

مثال : أوجد القاسم المشترك الأعظم 132 و 55 باستخدام خوارزمية أقليدس :

$$132 = 55 * 2 + 22$$
$$55 = 22 * 2 + 11$$
$$22 = 11 * 2 + 0$$

نتوقف عند الوصول إلى الصفر ، ويكون القاسم المشترك الأعظم هو 11 وذلك :

GCD(132,55) = GCD(55,22) = GCD(22,11) = GCD(11,0) = 11

gcd(55, 22) = gcd(22, 55 mod 22) = gcd(22, 11) = 11

مثال أخر : أوجد GCD (252,198) باستخدام خوارزمية أقليدس ؟

$$252 = 198 * 1 + 54$$
$$198 = 54 * 3 + 36$$
$$54 = 36 * 1 + 18$$
$$36 = 18 * 2 + 0$$

نتوقف عند الصفر ، والقاسم هو 18

GCD(252,198) = (198,54) = (54,36) = (36,18) = (18,0) = 18

الـ MOD الرياضي

إذا كان لدينا عدد موجب هو n وأي رقم آخر a، فإذا قسمنا a على n، فإننا نحصل على رقم ناتج القسمة هو q ورقم باقي القسمة هو r والذي يحقق العلاقة التالية:

$A = qn + r \quad 0 \leq r < n; \quad q = a/n$

مثال:

$A = 11; \quad n = 7; \quad 11 = 1 * 7 + 4; \quad r = 4$

$A = -11; \quad n = 7; \quad -11 = (-2) * 7 + 3; \; r = 3$

$11 \bmod 7 = 4; \quad -11 \bmod 7 = 3;$

عددين هما a و b يقال لهما باقيا القسمة إلى n،

وإذا كان.(a mod n) = (b mod n)

فإنها تكتب كما يلي $a \equiv b \bmod n.$

$37 \equiv 4 \bmod 23; \quad 21 \equiv -9 \bmod 10$

خصائص معامل باقي القسمة:

لمعامل باقي القسمة الخصائص التالية:

$a \equiv b \bmod n \quad$ if $\quad n \mid (a-b).$

1- $a \equiv b \bmod n$ implies $b \equiv a \bmod n.$

2- $a \equiv b \bmod n$ and $b \equiv c \bmod n$ imply $a \equiv c \bmod n$

مثال:

$23 \equiv 8 \pmod 5$ because $23-8 = 15 = 5*3$

$-11 \equiv 5 \pmod 8$ because $-11-5=-16=8*(-2)$

$81 \equiv 0 \pmod{27}$ because $81-0 = 81 = 27*3$

العمليات الرياضية لباقي القسمة:

تتضمن عمليات حساب باقي القسمة الميزات التالية:

1- [(a mod n)]+(b mod n)] mod n =(a + b) mod n

2- [(a mod n)]-(b mod n)] mod n =(a - b) mod n

3- [(a mod n)]*(b mod n)] mod n =(a *b) mod n

مثال:

11 mod 8 =3;   15 mod 8 =7

[(11 mod 8)+(15 mod 8)] mod 8 =10 mod 8 =2

(11+15) mod 8 = 26 mod 8 =2

[(11 mod 8)-(15 mod 8)] mod 8 = -4 mod 8 =4

(11-15) mod 8 = -4 mod 8 =4

[(11 mod 8)*(15 mod 8)] mod 8=21 mod 8 =5

(11*15) mod 8 = 165 mod 8 = 5

مثال:

لإيجاد قيمة المعادلة التالية 11^7 mod 13

11^7 mod 13

$11^2 = 121 \equiv 4$ mod 13

$11^4 = 4^2 \equiv 3$ mod 13

$11^7 = 11*4*3 \equiv 132 \equiv 2$ mod 13 = 2

الخوارزمية الإقليدية الممتدة Extended Euclidean Algorithm

يمكن تمثيل القاسم المشترك الأعظم للعددين عن طريق دمج خطي Linear Combination مع عددين آخرين ، وذلك كالتالي : GCD(x,y) = m*x + n*y

كيف يمكن أيجاد قيمتي n و m وذلك عن طريق خوارزمية اقليدس الممتدة .

يمكن أن نطلق عليها طريقة التراجع

لاحظ المثال التالي :

قم بتمثيل (GCD(26,21 :كـ Linear Combination للعددين 26 و 21 :

نبدأ في الحل كما هو الحال في طريقة اقليدس :

$$26 = 21 * 1 + 5$$
$$21 = 5 * 4 + 1$$
$$5 = 1 * 5 + 0$$

ونتوقف عند الصفر . الآن المعادلة التي قبل المعادلة التي باقيها صفر (وهي في حالتنا هذه المعادلة الثانية) نقوم بكتابتها بهذا الشكل :

$$1 = 21 - 4 * 5 \ldots\ldots\ldots\ldots [1]$$

أيضا المعادلة الأولى بنفس الشكل :

$$5 = 26 - 1 * 21 \ldots\ldots\ldots\ldots [2]$$

الآن نعوض المعادلة [2] في [1]

$$1 = 21 - 4 * (26 - 1 * 21)$$

ومن غير أجراء عملية حسابية ، فقط نفك القوس لينتج :

$$1 = 21 - 4 * 26 + 4 * 21$$

نجمع 21+21*4 ليكون لدينا الناتج النهائي :

$$= 5 * 21 + (-4) * 26$$

نتأكد من النتيجة، 5*21 + -4* 26 والناتج يساوي واحد ، اذا المعادلة صحيحة .

. اذا قيمة m هي 5 وقيمة n هي 4−

(حيث ان m, n يسمى معكوس العدد).

مثال : أوجد معكوس المعادلة $a = 3\ MOD\ 26$

الحل ، أولا نقوم بتطبيق خوارزمية اقليدس الممتدة ، على العددين 3 و 26 . كالتالي :

$$26 = 3 * 8 + 2 \;--\to 2 = 26 - 3 * 8$$

$$3 = 2 * 1 + 1 \;---> 1 = 3 - 2$$

$$2 = 1 * 2 + 0$$

$$1 = 3 - 2 = 3 - (26 - 8 * 3) = 3 - 26 + 8 * 3$$

$$= 9 * 3 - 26$$

$$1 = 9*3+(-1)*26$$

الآن العدد المجاور ل 3 هو المعكوس ، وهو 9

Lecture 06

- شفره أتباش Atbash Cipher

هذه الشفرة أيضا من أبسط أنواع الشفرات ، وهي كانت في الأصل للغة العبرية ، ولكن يمكن استخدام المفهوم في باقي اللغات .

وطريقتها كالتالي ، وهي أن نجعل الحرف الأول في اللغة هو الحرف الأخير ، والحرف الثاني هو قبل الأخير ، وهكذا...

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: ZYXWVUTSRQPONMLKJIHGFEDCBA

مثلا ، لتشفير الكلمة money يصبح لدينا الناتج nlmvb

في بعض الأحيان من الممكن أن الكلمات بعد التشفير يكون لديها معني وهي مشفره مثل:

النص الأصلي = "hob" ، بعد التشفير تصبح "sly" وهكذا للكلمات الأخرى

النص الأصلي= "hold" بعد التشفير تصبح"slow"

النص الأصلي = "holy" بعد التشفير تصبح "slob"

"horn" = "slim"

"irk" = "rip"

"low" = "old"

"glow" = "told"

"grog" = "tilt".

ومع ذلك تبقى تلك الشفرات من أسهل الأنواع على الإطلاق!

- شفره ROT13

هنا التشفير وفك التشفير يتم بنفس الطريقة ، و مفتاح التشفير 13 ، وللتشفير نقوم بجمع 13 على الحرف الأول من النص الأصلي ، ولفك التشفير تقوم أيضا بجمع 13 على الحرف الأول من النص المشفر .

P = ROT13 (ROT13 (P))

، الحرفp يعني الحرف الأول من النص الأصلي Plaintext نقوم بعدها بتشفيره بجمع 13 حرف إليه لنفرض أن الحرف الأول من النص الأصلي هوD الحرفD قيمته 3 نجمع (3+13)%26 والناتج هو 16 أو ممكن نتحرك 13 خطوه من الحرف D والناتج في النهاية ، سواء بالجمع أو بالتحرك هو الحرفQ .

قبل أن نبدأ عملية التشفير دائما ، نضع هذا الجدول الذي سنستخدمه كثيرا لتسهيل معرفة مواقع الحروف:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

عملية فك التشفير ، تكون أيضا بجمع 13 إلى الحرف المشفر (أو التحرك 13 خطوه إلى الأمام) نجرب على الحرف Q الذي كان نتيجة عملية التشفير السابقة ، (16+13)%26 =3.
أو نتحرك 13 خطوه إلى الأمام حتى نصل إلى الحرف الأصلي وهو.

- شفره Affine Cipher

Definition 1.4.4 Affine Cipher
Let $x, y, a, b \in \mathbb{Z}_{26}$
Encryption: $e_k(x) = y \equiv a \cdot x + b \bmod 26.$
Decryption: $d_k(y) = x \equiv a^{-1} \cdot (y - b) \bmod 26.$
with the key: $k = (a, b)$, *which has the restriction:* $\gcd(a, 26) = 1$.

التشفير بطريقة **Affine Cipher** البعض يترجمها بطريقة التشفير المختلط ، لأنه هنا خلط (بين نوعين من التشفير ، النوع الأول وهو شفره قيصر ، والأخر وهو شفره الضرب **product Cipher**.

في شفره قيصر يكون التشفير كالتالي :

$$c = p + key\ MOD\ n$$

. (وهنا**key** يعتبر الازاحه)

وفي شفره الضرب ، يكون التشفير كالتالي :

$$C = p * key\ MOD\ n$$

الآن في شفره **Affine** جمعت بين الطريقين ، حيث يتم الجمع والضرب أيضا

$$C = m * p + key\ MOD\ n$$

لكن هناك شرط مهم جدا وهو أن تكون **n** و **m** هما أوليان فيما بينهما ، أي أن القاسم المشترك ، الأعظم ل **n** و **m** يساوي **1** . وفي حال لم ينفذ هذا الشرط ، فانه لا يمكن فك التشفير.

الآن لفك التشفير يجب أن نوجد معكوس **m** في حال كان **GCD(m,n) =1** فإنه يمكن أيجاد ذلك المعكوس.

لفك التشفير ، نتبع :

$$P = m^{-1} * (c - key)\ (MOD\ n)$$

مثال:

نريد تشفير العبارة: **WAR LOST**

والمفتاح**key** يساوي **10** ومعامل الضرب **m** يساوي**5**

قبل أن نبدأ في التشفير ، يجب أن نتأكد من ان هناك معكوس لـm حتى يمكن فك الشفره

نأخذ القاسم المشترك الأعظم لـn و m

(26 لأنها عدد الحروف) .

GCD(5,26) = 1.

نضع جدول الحروف ، حتى يساعدنا في معرفة موقع الحروف :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

الآن بعد تحويل النص الأصلي إلى أرقام ، يكون بهذا الشكل :

19 18 14 11 17 0 22

الآن نبدأ في التطبيق في القانون :

$$C = m * p + key \text{ MOD } 26$$

$$C1 = 5 * 22 + 10 \text{ MOD } 26 = 16$$

$$C2 = 5 * 0 + 10 \text{ MOD } 26 = 10$$

$$C3 = 5 * 17 + 10 \text{ MOD } 26 = 17$$

$$C4 = 5 * 11 + 10 \text{ MOD } 26 = 13$$

$$C5 = 5 * 14 + 10 \text{ MOD } 26 = 2$$

$$C6 = 5 * 18 + 10 \text{ MOD } 26 = 22$$

$$C7 = 5 * 19 + 10 \text{ MOD } 26 = 1$$

الآن النتيجة بعد التشفير هي:

16 10 17 13 2 22 1

ونقوم بتحويلها إلى حروف ، ليصبح لدينا QKR NCWB :

الآن لفك التشفير ، يجب أن نعرف ما هو معكوس m حتى نستطيع التطبيق في القانون التالي : ،

$$P = m^{-1} * (c - key) \text{ (MOD } 26)$$

كيف يمكن إيجاد المعكوس ، وذلك عن طريق خوارزمية اقليدس الممتدة

ندخل العددين 5 و 26 في خوارزمية اقليدس الاقليدية الممتدة ، لينتج لدينا المعكوس :

الآن نطبق في القانون :

P1 = 21 * (16 – 10) MOD 26 = 22

P2 = 21 * (10 – 10) MOD 26 = 0

P3 = 21 * (17 – 10) MOD 26 = 17

P4 = 21 * (13 – 10) MOD 26 = 11

P5 = 21 * (2 – 10) MOD 26 = 14

P6 = 21 * (22 – 10) MOD 26 = 18

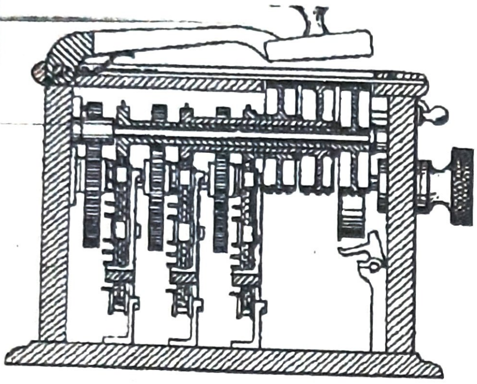
P7 = 21 * (1 – 10) MOD 26 = 19

اذا النص الأصلي هو 19 18 14 11 17 0 22 :وبعد تحويله إلى حروف يصبح

WAR LOST(وهو المطلوب)

Lecture 07

خوارزمية هيل HillCipher



- خوارزمية هيل Hill Cipher
  - مخترعها هو العالم (Lester S. Hill) ليستر هيل سنة 1929
  - تعتمد على علم «الجبر الخطي» Linear Algebra
  - تستخدم حرفان فأكثر لتشفير الحرف الواحد
  - استخدمت في الحرب العالمية الثانية
  - تستخدم لإخفاء خصائص اللغة
  - يمكن تنفيذها على أجهزة خاصة كما في الصورة المقابلة

- التشفير Encryption
  - كل حرف يمثل برقم Modulo 26, بالعادة يكون على شكل الجدول ادناه (يمكن استخدام قيم اخرى)
  - كل مجموع من الأحرف طولها (س) أي طول أكثر من 3 أحرف تعرف بأنها متجه vector
  - يتم ضرب المتجه vector بمصفوفة matrix (n*n) Modulus 26 ص*ص, هذه المصفوفةmatrix يجب أن يكون لها معكوس (n^{-1}) invers
  - **فك التشفير يكون عكس التشفير حيث يجب ضرب الناتج بمعكوس المصفوفة (n^{-1}) mod 26**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- التشفير Encryption بناء المصفوفة
  - افرض أن مفتاح التشفير هو GYBNQKURP
  - من الجدول نلاحظ القيم المقابلة لمفتاح التشفير
  - نبني المصفوفة المقابلة لهذه القيم (لابد أن يكون هناك معكوس للمصفوفة)

G	Y	B	N	Q	K	U	R	P
6	24	1	13	16	10	20	17	15

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- التشفير Encryption نص التشفير
  - مثال 1
  - على فرض أننا نود تشفير كلمة ACT
    - من الجدول نلاحظ القيم المقابلة لكلمة ACT
    - نبني المتجه المقابل للنص Vector

A	C	T
0	2	19

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- التشفير Encryption عملية التشفير

- For m=3:
- $C_1=(k_{11}p_1,+k_{12}p_2+k_{13}p_3)$ mod 26 : (6*0 + 24*2 + 1*19) =67
- $C_2=(k_{21}p_1,+k_{22}p_2+k_{23}p_3)$ mod 26 : (13*0 + 16*2 + 10*19) =222
- $C_3=(k_{31}p_1,+k_{32}p_2+k_{33}p_3)$ mod 26: (20*0 + 17*2 + 15*19) =319
- C=kp mod 26

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

- نتيجة التشفير هي الأرقام الناتجة
- بالنظر إلى الجدول نجد ان تشفير كلمة ACT هو POH

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

Note that:

67 mod 26 =15=P

222 mod 26=14=O

319 mod 26=7=H

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- مثال 2
- على فرض تشفير كلمة CAT وليس ACT كما في المثال السابق فإن التشفير لها يكون FIN

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

Note that:

31mod 26 =5=F

216 mod 26=8=I

325 mod 26=13=N

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- فك التشفير **Decryption**
- **نحتاج إلى معرفة معكوس المصفوفة n^{-1} matrix**
- معكوس المصفوفة هو IFKVIVVMI

- $C=E_k(P)= KP \bmod 26$
- $P=D_k(C)= K^{-1}C \bmod 26 = K^{-1}KP = P$
- $C_3=(k_{31}p_1,+k_{32}p_2+k_{33}p_3) \bmod 26$

- فك التشفير Decryption
- حساب Matrix Inverse

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \pmod{26}$$

- نستخدم النص المشفر السابق POH

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

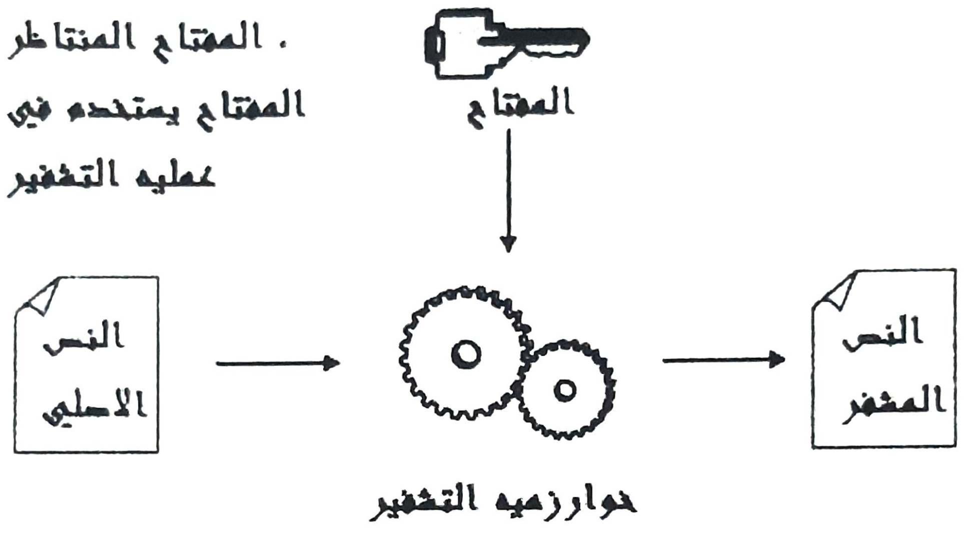
- النتيجة 0 2 19 وتقابل النص الأصلي قبل التشفير ACT

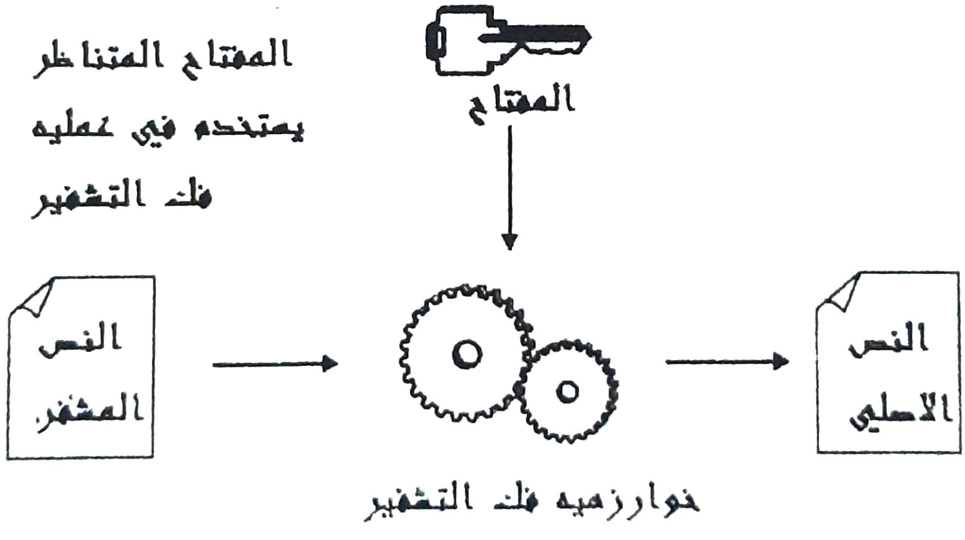
Lecture 08

- التشفير بالمفتاح المتناظر: Symmetric key Cryptography

وهنا سوف نستخدم مفتاح مع خوارزمية ، وسوف نستخدم نفس المفتاح ونفس الخوارزمية لفك التشفير .

في التشفير بالمفتاح المتناظرSymmetric المفتاح الذي يستخدم للتشفير هو نفسه الذي يستخدم لفك التشفير ، ومن هنا جاءت كلمة المتناظر(أو المتماثل) ، يعني هو نفسه من الطرفين ، الصوره التالية توضح العملية :





لاحظ انه في حالة شفرت الرسالة بخوارزمية معينة (مثلاDES) ، ومفتاح معين (مثلا 10)

الآن في حالة فك التشفير يجب أن استخدم نفس الخوارزمية ونفس المفتاح والا فلن احصل على النص الأصلي.

- الهجوم على البيانات المشفرةAttacks on Encrypted Data

المخترق هو الشخص الذي يريد سرقة المعلومات ، ولكي يحصل على المعلومات يجب أن يفك تشفير البيانات المشفرة ، ولفك التشفير فإن لدىه طريقتان ، معرفه المفتاح ، أو كسر الخوارزمية .

- الهجوم على المفتاح Attacks on Keys:

وطريقته هو أن brute-force attack هنا يقوم المخترق بتطبيق هجوم يسمى القوه العنيفة يجرب مفتاح مفتاح إلى أن يصل إلى المفتاح المطلوب.

هناك نوعين من أنواع التشفير بالمفتاح المتناظر

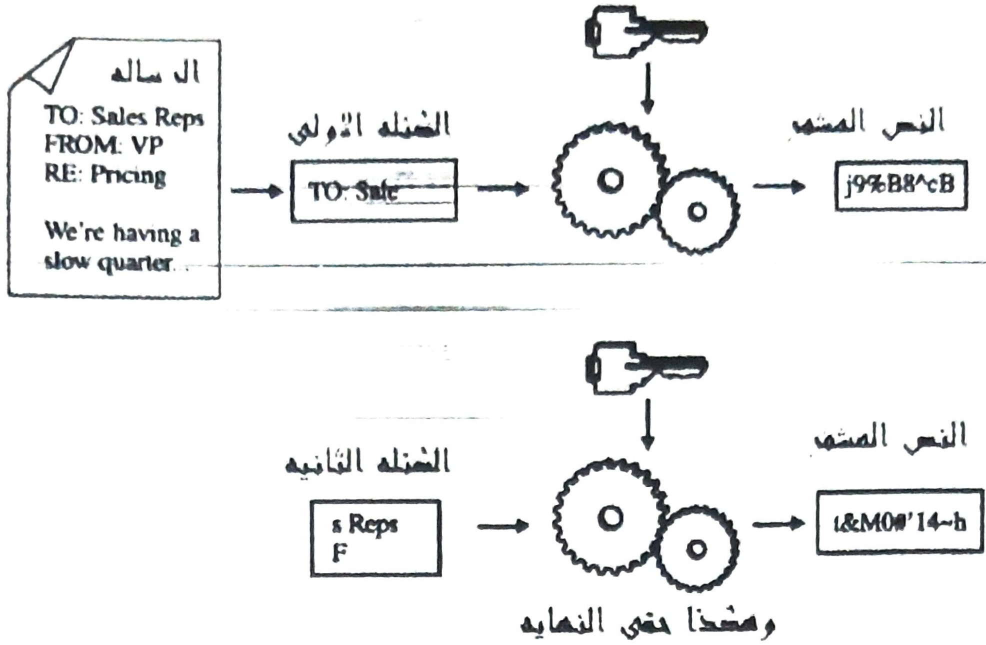
وهما :

*شفرات الكتلBlock Cipher

*شفرات التدفقStream Cipher

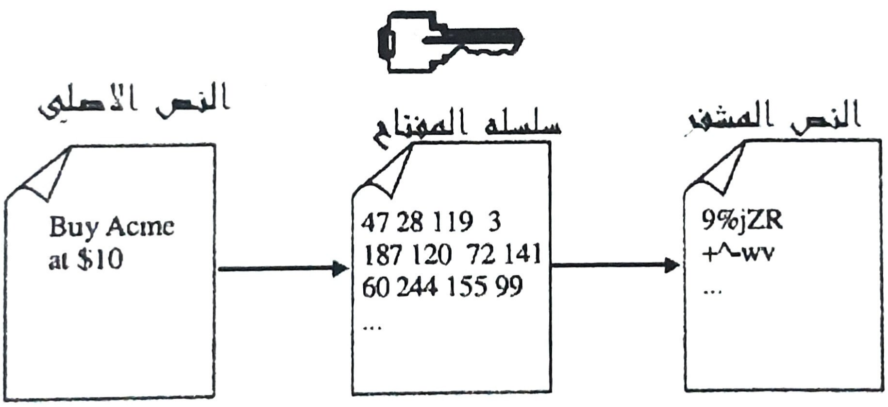
- شفرات الكتلBlock Cipher

شفرات الكتل (كما هو واضح من اسمها) تعمل علىBlock كتلة(من البيانات في كل مره) عندما تزود الخوارزمية (أو برنامج التشفير) بالنص الأصلي هنا في هذا النوع يقوم بتقسيم النص إلى عده من الكتل ، كل كتلة حجمها يكون 64 بت وأحيانا 128 بت (16 بايت) ، طبعا الحجم بيكون على حسب الخوارزمية المستخدمة



- شفره التدفقStream Ciphers

النوع الثاني من أنواع التشفير بالمفتاح المتناظر هو شفره التدفق ، وهنا سوف نتعامل مع بت بت من الممكن أن تعتمد على Key Stream أو بايت بايت وليس كتلة كتلة ، وعملية توليد المفتاح النص المشفر السابق ومن الممكن لا (هناك نوعين من هذا النوع ، نوع متزامن ونوع غير متزامن) .



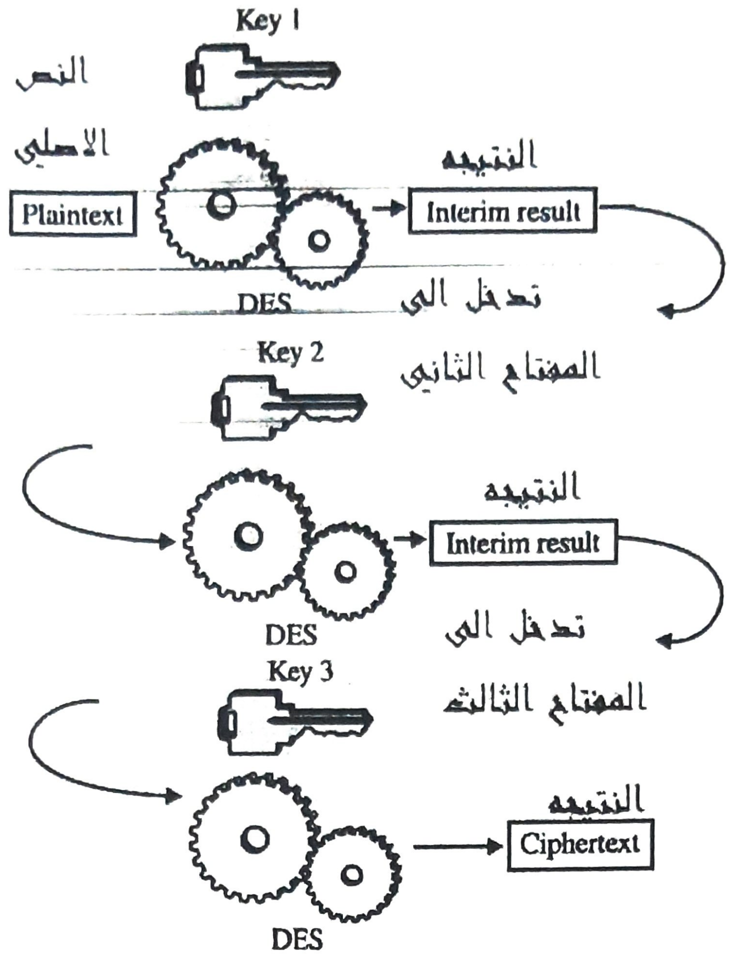
Digital Encryption Standard -

في بداية السبعينات تم معرفة انه اغلب الشفرات القديمة لم تعد مجدية وغير نافعة للتشفير ، ولهذا قرر علماء في شركة IBM بعمل خوارزمية جديدة للتشفير تبنى على بنية قديمة تسمى Lucifer (Horst Feistel نسبة إلى مخترعها)ومن خلال مساعده وكالة الأمن القومي NSA ، . تم عمل خوارزمية DES.

DES هي احد شفرات الكتل Block Cipher وتأخذ مفتاح بطول 56 بت ، وتعمل على كتلة ، طولها 64 بت .

Triple DES -

احد البدائل كانت خوارزميةTriple DES ، أو البعض يسموها 3DES هي بكل بساطة DES ولكن ثلاثة مرات ، يعني سوف تدخل الكتلة الأولى (16 بايت) إلى الخوارزمية بالمفتاح الأول ، والناتج سوف يدخل إلى الخوارزمية مع المفتاح الثاني ، والناتج سوف يدخل مع المفتاح الثالث .



هنا سوف نستخدم ثلاثة مفاتيح ، كل منها بطول 56 بت

تم اعتماد طول المفتاح ليكون 64 بت ولكن يستعمل منها فقط 56 بت فقط بشكل فعال وتستعمل الباقية كخانات تدقيق للأخطاء ، وبما أن الخوارزمية متناظرة يستعمل نفس المفتاح للتشفير وفك التشفير وبالرغم من إمكانية اختراق خوارزمية DES فإنها مازالت تستخدم بشكل كبير ولكن تم استبدالها في الآونة الأخيرة بخوارزمية Treble DES حيث يتم تطبيق خوارزمية DES ثلاث مرات بمفاتيح مختلفة. ويوجد عدة إصدارات لخوارزمية DES وهي

SDES

STANDAR (DES)

SDES(simple Data Encryption Standard:)

DOUBL DES

TRUBLE DES

سوف نتوسع في شرح هذا النوع من التشفير في خوارزمية DES لأنه ابسط نوع من هذه الأنواع وسوف يكون تعاملنا في شرح مثال عن الخوارزمية باستخدام النظام الثنائي

ويجب ان نفهم بعض المصطلحات او التعاريف لنبدأ بعملية التشفير

1- Initial Permutation (IP) : وهي التبديل المبدئي للبيانات المراد تشفيرها و وظيفتها ادخال 8بت نقوم بتغير اماكنها بشكل غير منظم بناءً على ارقام تم تحديدها بطلبنا وتكون من رقم 1 إلى 8 ولكن هذه الأرقام غير مرتبة.

ملاحظة:

$$EP= \left.\begin{matrix} n_4 \\ n_2 \end{matrix}\right| \begin{matrix} n_1 & n_2 \\ n_3 & n_4 \end{matrix} \left|\begin{matrix} n_3 \\ n_1 \end{matrix}\right.$$

Calculate S0, S1

The first 4 bits (first row of the preceding matrix) are fed into the S-box S0 to produce a 2-bit output, and the remaining 4 bits (second row) are fed into S1 to produce another 2-bit output. These two boxes are defined as follows:

$$S0 = \begin{matrix} & 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{matrix} \qquad S1 = \begin{matrix} & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{matrix}$$

The S-boxes operate as follows. The first and fourth input bits are treated as a 2-bit number that specify a row of the S-box, and the second and third input bits specify a column of the Sbox.

The entry in that row and column, in base 2, is the 2-bit output.

- مثال:

باستخدام خوارزمية SDES قم بتوليد المفتاحين K1,K2 وفقا للمعطيات التالية؟

P10									
3	5	2	7	4	10	1	9	8	6

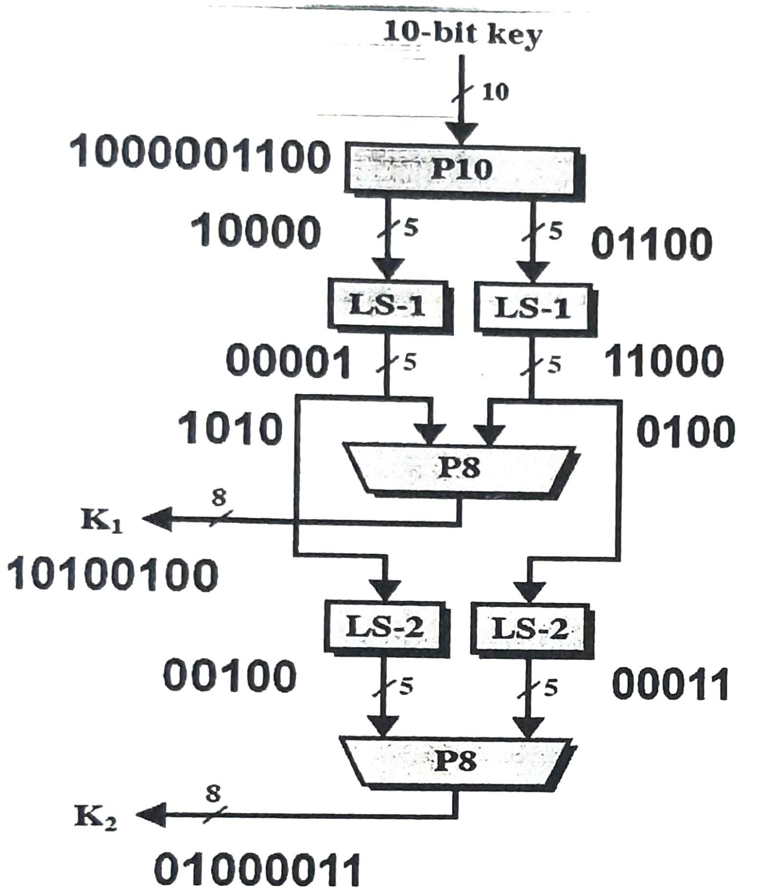
P8							
6	3	7	4	8	5	10	9

- Key Generation

the key (1010000010)

P10

3	5	2	7	4	10	1	9	8	6



Key Generation for Simplified DES

P8

6	3	7	4	8	5	10	9

P8

6	3	7	4	8	5	10	9

مثال2:

باستخدام خوارزمية SDES قم بتوليد المفتاحين K1,K2 ثم قم بعملية التشفير باستخدام K1 فقط وفقا للمعطيات التالية

PLAINTEXT "6Ch"

KEY "B9&11"

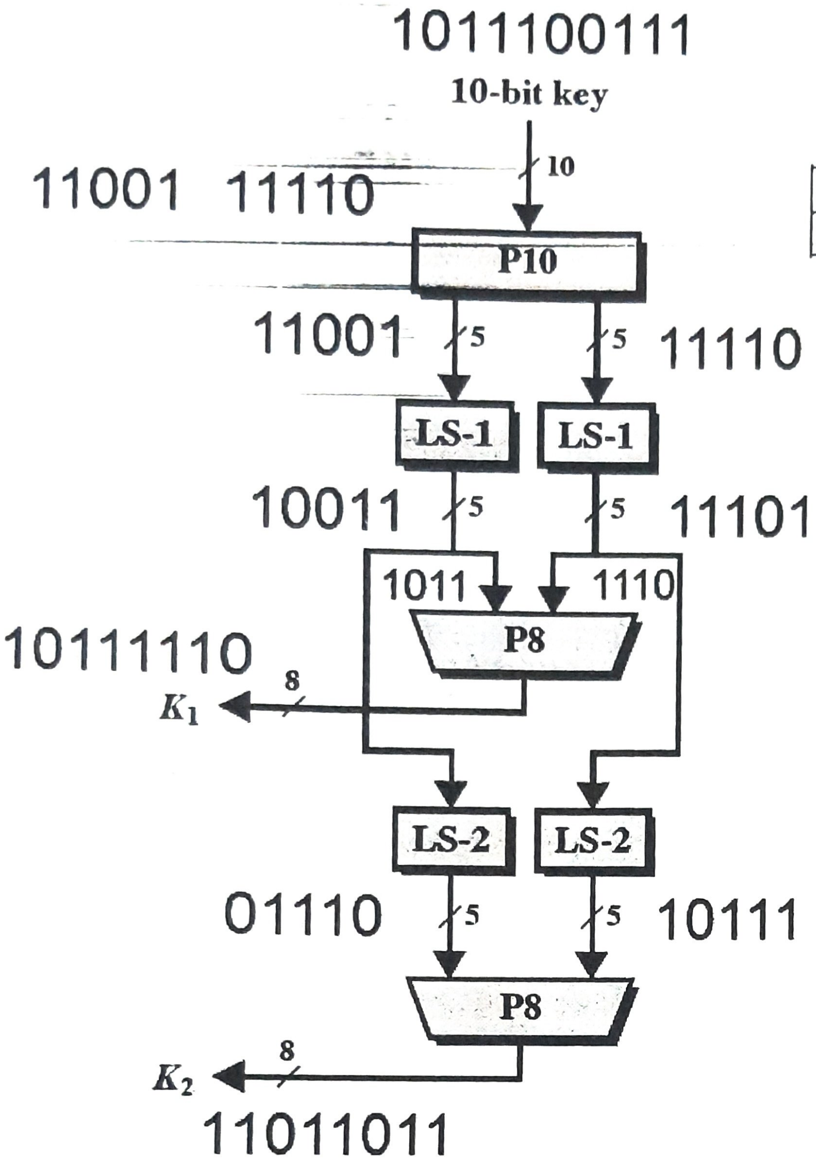
IP							
2	6	3	1	4	8	5	7

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

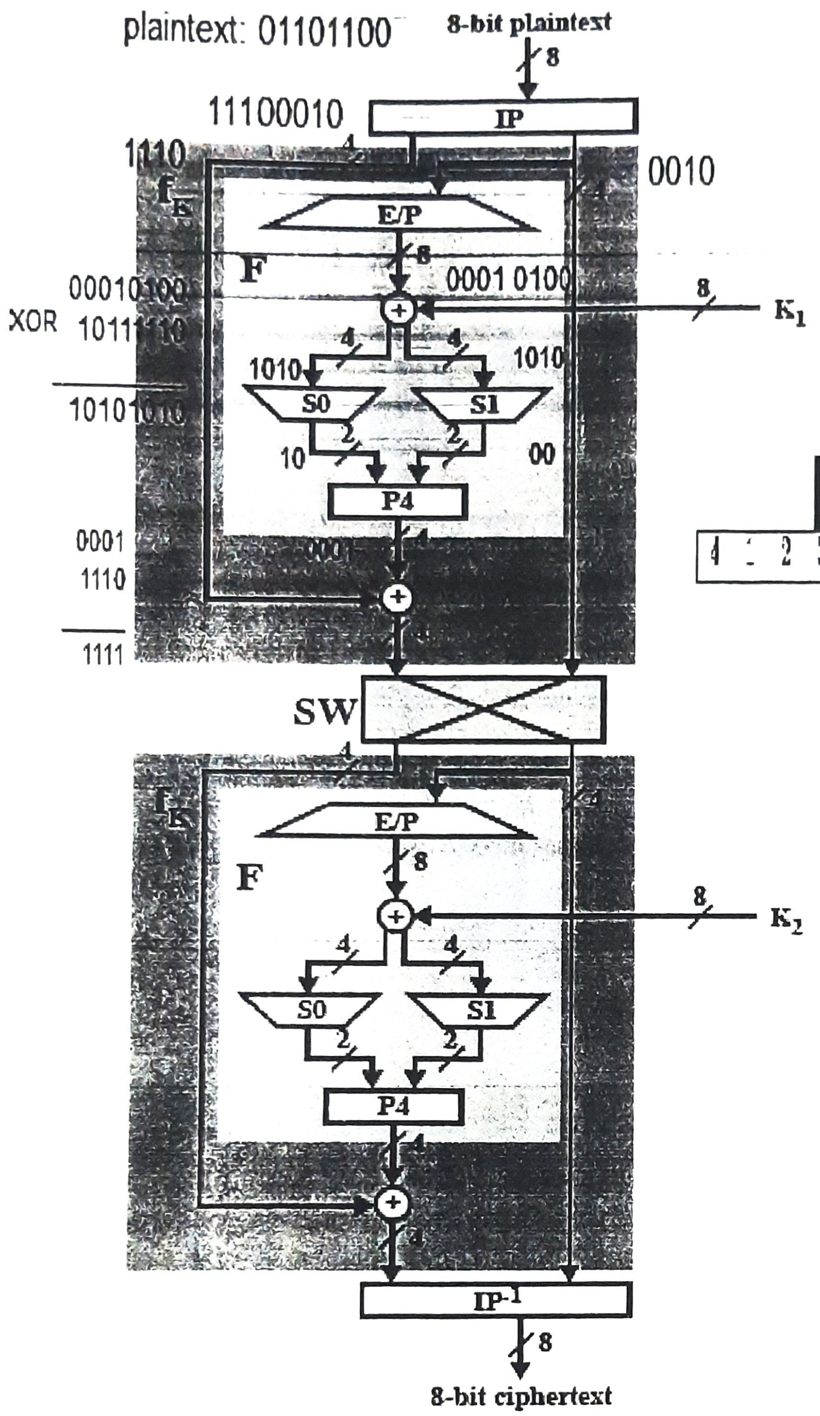
P4			
2	4	3	1

$$S0 = \begin{matrix} & \begin{matrix} 0 & 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{matrix} \qquad S1 = \begin{matrix} & \begin{matrix} 0 & 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{matrix}$$



P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9



IP

2	6	3	1	4	8	5	7

IP^{-1}

4	1	3	5	7	2	8	6

P4

2	4	3	1

EP

4	1	2	3	2	3	4	1

$$S0 = \begin{matrix} & 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{matrix} \qquad S1 = \begin{matrix} & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{matrix}$$

CIPHER TEXT = "2Fh"